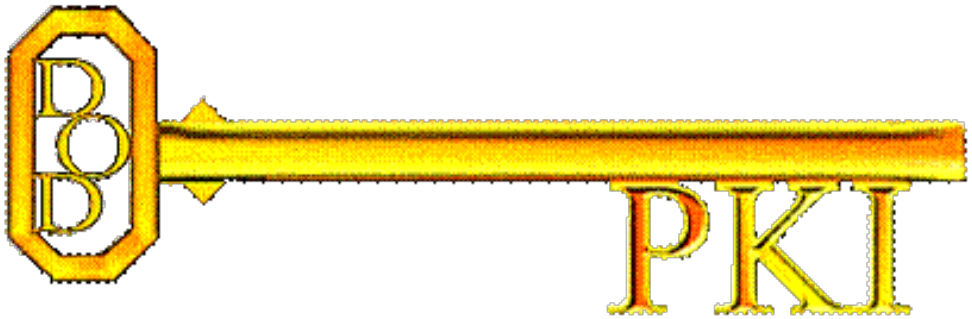
2016
Major Automated Information System
Annual Report



Public Key Infrastructure Increment 2 (PKI Inc 2)

Defense Acquisition Management
Information Retrieval
(DAMIR)

Table of Contents

Common Acronyms and Abbreviations for MAIS Programs 3
Program Information 4
Responsible Office 4
References 4
Program Description 5
Business Case 6
Program Status 7
Schedule 8
Performance 9
Cost 12

Common Acronyms and Abbreviations for MAIS Programs

Acq O&M - Acquisition-Related Operations and Maintenance
ADM - Acquisition Decision Memorandum
AoA - Analysis of Alternatives
ATO - Authority To Operate
APB - Acquisition Program Baseline
BY - Base Year
CAE - Component Acquisition Executive
CDD - Capability Development Document
CPD - Capability Production Document
DAE - Defense Acquisition Executive
DoD - Department of Defense
DoDAF - DoD Architecture Framework
FD - Full Deployment
FDD - Full Deployment Decision
FY - Fiscal Year
IA - Information Assurance
IATO - Interim Authority to Operate
ICD - Initial Capability Document
IEA - Information Enterprise Architecture
IOC - Initial Operational Capability
IP - Internet Protocol
IT - Information Technology
KPP - Key Performance Parameter
$M - Millions of Dollars
MAIS - Major Automated Information System
MAIS OE - MAIS Original Estimate
MAR – MAIS Annual Report
MDA - Milestone Decision Authority
MDD - Materiel Development Decision
MILCON - Military Construction
MS - Milestone
N/A - Not Applicable
O&S - Operating and Support
OSD - Office of the Secretary of Defense
PB - President’s Budget
RDT&E - Research, Development, Test, and Evaluation
SAE - Service Acquisition Executive
TBD - To Be Determined
TY - Then Year
U.S.C- United States Code
USD(AT&L) - Under Secretary of Defense for Acquisition, Technology, & Logistics

Program Information

Program Name

Public Key Infrastructure Increment 2 (PKI Inc 2)

DoD Component

DoD

The acquiring DoD Component is the National Security Agency

Responsible Office

Program Manager

Mr. Charles Huskey
DoD PKI Program Management Office
9800 Savage Road
Suite 6718
Fort Meade, MD, MD 20755

Phone: 410-854-4699
Fax: 240-373-6615
DSN Phone: 244-4900
DSN Fax:
Date Assigned: July 1, 2015

cthuske@nsa.gov

Ms. Karen Clay
Deputy Program Manager
410-854-4661
9800 Savage Road
Suite 6718
Fort Meade, MD 20744-6718

References

MAIS Original Estimate

October 24, 2015

Approved APB

Defense Acquisition Executive (DAE) Approved Acquisition Program Baseline (APB) dated July 24, 2015

Program Description

A Public Key Infrastructure (PKI) is a critical enabling technology for Information Assurance (IA) services to support seamless secure information flows across the Global Information Grid (GIG) and at rest. Using authoritative data, obtained via face-to-face identity proofing, PKI creates a credential that combines this identity information with cryptographic information that is non-forgeable and non-changeable. In this way, PKI provides a standards-based representation of a physical identity in an electronic form. With this PKI-based identity, data sharing amongst appropriate, broad, and dynamic Communities of Interest (COI) will be enabled. PKI IA services enable and promote a common ubiquitous secure web-services environment; it allows war fighters and other authorized users to securely access, process, store, transport, and use information, applications and networks regardless of technology, organization, or location. PKI enables the integrity of data/forms/orders moving within the GIG, via use of digital signatures. PKI enables management of identities operating in groups or certain roles within GIG systems. PKI can also ensure the integrity and confidentiality of what is operating on a network by provision of assured PKI-based credentials for any device on that network.

PKI Increment One made significant improvements to the capability for use on the Non-Secure Internet Protocol Router Network (NIPRNet) using a Common Access Card (CAC) for users throughout DoD and the Federal Government. The CAC contains the trusted certificates that allows for the secure exchange of information throughout the unclassified network.

PKI Increment Two, Spirals One and Two, provided similar capabilities on the Secret Internet Protocol Router Network (SIPRNet) environment using an approved SIPRNet token (versus a CAC). The Token Management System (TMS), a key component of the PKI, was engineered and developed to provide a distributed capability for the management, reporting, generation, recovery, administration, and control of SIPRNet tokens.

PKI Increment Two Spiral 3 includes further enhancements to TMS that will be developed and implemented through a series of program releases.

PKI Increment Two Spiral 4 will include new capabilities such as the NIPRNet Enterprise Alternate Token System (NEATS) and enhancements to the Non-Person Entity (NPE) system that operates in the NIPRNet and SIPRNet environments.

Business Case

Business Case Analysis, including the Analysis of Alternatives: Guidance for the DoD PKI Increment 2 AoA was issued May 1, 2006, and a Plan for the analysis was approved on July 14, 2006. The ensuing AoA considered a Status Quo alternative; Enhanced Status Quo alternatives; Personal Identity Verification of Federal Employees and Contractors (HSPD-12 and Federal Information Processing Standards (FIPS) 201) alternatives; PKI for SIPRNET and/or SIPRNET applications and collateral classified networks alternatives; and austere and tactical environments alternatives. In August 2008 the DoD PKI Increment 2 Economic Analysis (EA) was approved, which identified the Life Cycle Cost Estimate in support of the DoD PKI. It examined the costs, benefits, schedule, and risks associated with the Status Quo and the recommendations of the DoD PKI AoA to implement PKI Enhancements and SIPRNET Expansion. The resulting analysis in the Enhanced Status Quo, SIPRNet, non-land force tactical environment, and alignment with HSPD-12 alternatives being approved by the MDA, in the “Public Key Infrastructure Increment 2 Acquisition Decision Memorandum,” dated April 30, 2009.

On October 31, 2013, the program determined a Critical Change was experienced due to a delay in achieving the FDD. The Critical Change Report was provided to Congress on July 11, 2014.

Firm, Fixed-Price Feasibility: The determination of the contract type was based on cost risk associated with the estimated cost of satisfying the requirement. PKI utilizes both firm, fixed-price and cost contracts. Where cost and technical risk of satisfying the requirements was sufficiently well understood, a firm, fixed-price contract was used to execute the middleware, SIPRNet tokens, and card readers in the program’s current acquisition phase. Additionally, the MDA selected a cost-type contract because development tasks were sufficiently complex and technically challenging that it was impossible to precisely estimate the cost of satisfying the requirements, and it was not practicable to reduce cost and technical risk to a level that would permit the use of a fixed-price contract.

Independent Cost Estimate: The Senior Official determined on October 31, 2013, that the program experienced a Critical Change due to a delay in achieving the FDD. To support the Critical Change Report, the NSA Cost Estimating organization prepared a cost estimate that was validated by the Director of Cost Assessment and Program Evaluation. The resulting cost estimate itself represents an increase in the life-cycle cost estimate exceeding the Critical Change threshold. The Original Estimate had not included the appropriate 10 years of sustainment costs.

Certification of Business Case Alignment: I certify that all technical and business requirements have been reviewed and validated to ensure alignment with the business case. This certification is based on my review of the AoA and EA described above and the Critical Change Report.

Business Case Certification:

Name:	Ms. Jennifer S. Walsmith
Organization:	National Security Agency for PKI Inc 2
CAC Subject:	CN=WALSMITH.JENNIFER.9000045983, OU=NSA/CSS, OU=PKI, OU=DOD, O=U.S. GOVERNMENT, C=US
Date:	3/17/2015 10:29 AM

Business Case Changes

No significant change to the Business Case and Certification.

Significant Change: The program is projecting a seven-month schedule delay for the achievement of the Full Deployment Decision. Per 10 U.S.C. Chapter 144A, the Senior Official will notify Congress of the Significant Change.

Program Status

Significant Change: The program is projecting a seven-month schedule delay for the achievement of the Full Deployment Decision. Per 10 U.S.C. Chapter 144A, the Senior Official will notify Congress of the Significant Change.

Schedule

Schedule Events		
Events	**Original Estimate Objective**	**Current Estimate (Or Actual)**
Funds First Obligated	Mar 2009	Mar 2009
Milestone A[1]	N/A	N/A
Milestone B	Apr 2009	Apr 2009
Milestone C	Feb 2011	Feb 2011
Full Deployment Decision	Sep 2017	Apr 2018
Full Deployment[2]	TBD	TBD

Memo

1/ The DoD PKI Increment Two entered the acquisition process at MS-B.

2/ In accordance with 10 U.S.C. Chapter 144A, the Full Deployment date is TBD until defined in the Full Deployment Decision Acquisition Decision Memorandum.

Acronyms and Abbreviations

TBD - To Be Determined

Performance

Performance Characteristics		
Original Estimate Objective/Threshold		**Current Estimate (Or Actual)**
Assured Issuance: DoD PKI shall support the assured issuance of certificates to support: 1. Authentication to information and network resources by individuals, whether in group/organizations or in a job function. 2. Integrity of information transmitted by individuals, whether in group/ organizations or in a job function. 3. Confidentiality of information transmitted by individuals, whether in group/organizations or in a job function. 4. Authoritative naming source for NPEs to support electronic key management. 5. NPE authentication to network resources. 6. Integrity of software used within or transmitted over DoD networks (i.e. mobile code,) and the provision of security services within the issuance process itself.		
Issue certificates (to include authorized subscriber renewal, modification, and re-key requests) for human, code-signing, and NPEs formatted in accordance with ITU Recommendation X.509 and as tailored in certificate profiles specified by the DoD CP, with 99.99% accuracy that the data entered is the data placed in the certificate and a response time of ten seconds.	Issue certificates (to include authorized subscriber renewal, modification, and re-key requests) for human, code-signing, and NPEs, formatted in accordance with International Telecommunications Union (ITU) Recommendation X.509 and as tailored in certificate profiles specified by the DoD Certificate Profile, with 99.9% accuracy that the data entered is the data placed in the certificate and a response time of 30 seconds.	Will meet Threshold.
Assured Validation/ Revocation 1.DoD PKI shall provide assured/secure validation of revocation of an electronic/ digital credential. 2.DoD PKI shall support assured revocation status requests of certificates within a network, as an enterprise and/or local enclave resource, to enable trust decisions regarding information transactions or authentication to network resources. 3.DoD PKI shall provide assured management of single or group certificate revocation processes to enable trust decisions for any information or network resource transaction. Specifically, in response to a notification of a private key compromise, PKI must issue a new CRL within the following time limits, where the response time is measured from the reception of the compromise notification by the CA to the posting of the new CRL for pull to the directory.		
Provide trusted methods, based on commercial standards, for real-time check of certificate revocation status with a response time of two seconds per revocation status request. Selected means for revocation status checking shall be supported by commercial applications and/or with commercial plug-ins. Provide the capability to publish revocation information by generating a new CRL for distribution every six hours, available for pull by DoD directories and RCVS within 15 minutes of compromise notice being received by CA for compromised subscribers. As needed, to revoke up to 30,000 certificates in a single request, with new CRLs generated within six hours of receipt of request and successfully made available to the master GDS within	Provide trusted method, based on commercial standards, for real-time check of certificate revocation status with a response time of five seconds per revocation status request. Selected means for revocation status checking shall be supported by commercial applications and/or with commercial plug-ins. Provide the capability to publish revocation information by generating a new CRL for distribution every 18 hours, available for pull by DoD directories and RCVS within six hours of compromise notice being received by CA for compromised subscribers. As needed, to revoke up to 10,000 certificates in a single request, with new CRLs generated within 18 hours of receipt of request and successfully made available to the master GDS within four hours after generation.	Will meet Threshold.

four hours after generation.		
Net-Centricity (Net-Ready) The system must support Net-Centric military operations. 1.The system must be able to enter and be managed in the network, and exchange data in a secure manner to enhance mission effectiveness. 2.The system must continuously provide survivable, interoperable, secure, and operationally effective information exchanges to enable a Net-Centric military capability.		
The system must fully support execution of all operational activities identified in the applicable joint and system integrated architectures and the system must satisfy the technical requirements for Net-Centric military operations to include: 1.DISR mandated GIG IT standards and profiles identified in the TV-1, 2.DISR mandated GIG KIPs identified in the KIP declaration table, 3.NCOW RM Enterprise Services 4.Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Approval to Operate (ATO) by the Designated Approval Authority (DAA), and 5.Operationally effective information exchanges; and mission critical performance and information assurance attributes, data correctness, data availability, and consistent data processing specified in the applicable joint and system integrated architecture views.	The system must fully support execution of joint critical operational activities identified in the applicable joint and system integrated architectures and the system must satisfy the technical requirements for transition to Net-Centric military operations to include: 1.DoD Information Technology Standards and Profile Registry (DISR) mandated GIG IT standards and profiles identified in the Technical View (TV)-1, 2.DISR mandated GIG Key Interface Profiles (KIPs) identified in the KIP declaration table, 3.Network Centric Operations and Warfare Reference Model (NCOW RM) Enterprise Services 4.Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Interim Approval to Operate (IATO) by the DAA, and 5.Operationally effective information exchanges; and mission critical performance and information assurance attributes, data correctness, data availability, and consistent data processing specified in the applicable joint and system integrated architecture views.	Will meet Threshold.
Materiel Availability (Sustainment) 1. The DoD PKI shall be available 24/7 to provide all services to both strategic and bandwidth constrained (i.e., tactical environment) users with no single points of failure. PKI operational availability is defined as the time that PKI is prepared to: a. Respond to requests to register subscribers; b. Generate new, modified or re-keyed certificates; c. Process revocation requests; d. Generate CRLs; e. Provide certificate status checking; and f. Respond to key recovery requests. 2. PKI shall provide an automated ability to archive and retrieve PKI-generated security objects on demand. Assured management of PKI-generated security objects that are automatically archived and recoverable on demand to prove subscriber's recognition of compliance to policies and validity of PKI enabled transactions.		
97% of DoD PKI's core component inventory on NIPRNet/SIPRNet, will be operationally capable at any time to performing an assigned task supporting PKI services. PKI services across the core infrastructure must be operationally available 99.99% of the time. PKI shall provide the ability to archive and retrieve the following PKI-generated security objects: PKI CA public key certificates; PKI subscriber public key certificates; PKI CRLs; PKI audit information as defined in the DoD CP Security objects archived for as many as 10 years, six months for a Medium Assurance PKI, and 20 years six months for a High Assurance PKI after the date of the transaction.	94% of DoD PKI's core component inventory on NIPRNet/SIPRNet will be operationally capable at any time to performing an assigned task supporting PKI services. PKI services across the core infrastructure must be operationally available 99.9% of the time. PKI shall provide the ability to archive and retrieve the following PKI-generated security objects: PKI CA public key certificates; PKI subscriber public key certificates; PKI CRLs; PKI audit information as defined in the DoD CP Security objects archived for as many as 10 years, six months for a Medium Assurance PKI, and 20 years six months for a High Assurance PKI after the date of the transaction.	Will meet Threshold.

Secure Information Exchange Assured use of certificates to support: a.Authentication to information and network resources discriminated by certificate policy/naming for individuals and organizations external to the US DoD; b.Integrity of information transactions discriminated by factors of certificate policy/naming for individuals and organizations external to the US DoD; and c.Confidentiality of information transactions with individuals and organizations external to the US DoD.		
Provide Federated interoperability within the Federal Government and close allies (e.g., CCEB and FBCA) via a common policy framework on NIPRNet and SIPRNet.	Provide interoperability within the Federal Government and close allies (e.g., CCEB and the Federal Bridge Certification Authority [FBCA]) via a common policy framework on the NIPRNet	This KPP was not validated by the Joint Requirements Oversight Council (JROC) as part of the Critical Change and will be deleted.

Memo

The Joint Staff J6 issued a memo in September 2014 acknowledging that the Secure Information Exchange KPP was never validated by the Joint Requirements Oversight Council. It is in the process of being removed from all program documentation.

Acronyms and Abbreviations

ATO - Approval To Operate
CA - Certificate Authority
CCEB - Combined Communications-Electronics Board
CP - Certificate Profile
CRL - Certificate Revocation List
DAA - Designated Approval Authority
DoD - Department of Defense
FBCA - Federal Bridge Certification Authority
GDS - Global Directory Service
IATO - Interim Approval To Operate
ITU - International Telecommunications Union
NCOW RM - Network Centric Operations and Warfare Reference Model
NIPRNet - Non-Secure Internet Protocol Router Network
NPE - Non-Person Entity
PKI - Public Key Infrastructure
RCVS - Robust Certificate Validation Service
SIPRNet - Secret Internet Protocol Router Network
TV - Technical View

Cost

PKI Inc 2				
Appropriation Category	BY 2015 $M		TY $M	
	Original Estimate	Current Estimate Or Actual	Original Estimate	Current Estimate Or Actual
Acquisition Cost				
RDT&E	134.1	178.1	134.9	180.6
Procurement	61.8	64.1	64.3	62.9
MILCON	0.0	0.0	0.0	0.0
Acq O&M	0.0	0.0	0.0	0.0
Total Acquisition Cost	195.9	242.2	199.2	243.5
Operating and Support (O&S) Cost				
Total Operating and Support (O&S) Cost	307.6	257.3	356.8	287.8
Total Life-Cycle Cost				
Total Life-Cycle Cost	503.5	499.5	556.0	531.3

Cost Notes

1. This report and the Budget Year IT-1 Exhibit cover different time periods thus the costs will not match.
2. Then Year dollars are included for information purposes only; cost variances will be reported against Base Year dollars.
3. The O&S costs reflect all work performed during that phase, regardless of the type or source of funding.

Cost Analysis and Program Evaluation (CAPE) Cost Memo signed by George N. Leo, Jr. (then NSA PM) and Robert Williams (DISA Chief, Analysis and Acquisition Support) on March 19, 2014, and Alec Salerno (NSA Chief, Cost Analysis and Research) and Jennifer Walsmith (NSA Senior Acquisition Executive) on March 20, 2014.

This APB establishes the following affordability caps for the PKI Inc 2 program (BY 2015 $M):
There is no Procurement affordability cap because the program has no procurement funding beyond FY 2015. Operating and Support: Is less than or equal to $29.6M, based on the average annual O&S cost in BY 2015 with a service life from 2019-2028.